IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

PHILLIPS MEDICAL SYSTEMS PUERTO RICO, INC., Plaintiff v. **GIS PARTNERS CORP.** *et al.*, Defendants.	Civil No. 15-2702 (GAG/BJM)

REPORT AND RECOMMENDATION

Phillips Medical Systems Puerto Rico, Inc. ("Phillips-PR") brought this action against GIS Partners Corp. ("GIS"), Hernan Toro ("Toro"), David Sumpter ("Sumpter"), and Radames Bracero ("Bracero"), alleging breach of contract, unfair competition, violation of four sections of the Computer Fraud and Abuse Act ("CFAA" or "Act"), 18 U.S.C. § 1030, and violation of Puerto Rico's Industrial and Trade Secret Protection Act, P.R. Laws Ann. tit. 10, §§ 4131–4141. Docket No. 38. Only the § 1030(a)(2) and state-law claims survived the motion to dismiss. Docket Nos. 76, 99. Phillips-PR moved for a preliminary injunction, Docket No. 2, and GIS, Toro, and Sumpter opposed.[1] Docket No. 53. This matter was referred to me for a report and recommendation, Docket No. 74, and an evidentiary hearing was held on July 29, 2016. Docket No. 96.

For the reasons set forth below, injunctive relief should be **GRANTED.**

BACKGROUND[2]

Phillips-PR, a subsidiary of Royal Phillips Electronics ("Phillips"), is a Puerto Rico corporation that sells and services medical equipment in Puerto Rico, such as

[1] Bracero did not pursue his opposition to the motion, as he and Phillips-PR reached a settlement agreement prior to the preliminary injunction hearing. Docket Nos. 89, 101.

[2] This account is based upon the testimony and evidence provided during the hearing, unopposed facts that Phillips-PR moved to have judicially noticed, Docket Nos. 92, 103, and the parties' stipulated facts (the ninth of which was re-disputed prior to the commencement of the preliminary injunction hearing). Docket No. 91.

magnetic resonance imaging ("MRI") machines. Docket No. 91 ¶¶ 1, 3. Edwin Calo-Rodriguez ("Calo") is Phillips-PR's country manager, in which capacity he oversees the sales division and the services provided to companies that have purchased Phillips-branded medical equipment. Calo testified that Phillips-PR employs field service engineers to service and repair Phillips-branded medical equipment. *Id.* ¶ 2. To perform their job functions, field service engineers must have certain pre-acquired skills in addition to the training they receive in Phillips's factories. After completing these trainings, field service engineers are provided hardware and software that belong to Phillips.

Toro, Sumpter, and Bracero are former employees of Phillips-PR. Toro served as a field service engineer of CT scan products for 15 years, and left the company in 2009. Sumpter worked as an equipment salesperson for 20 years, and also left the company in 2009. Docket No. 92 ¶¶ B, C. Bracero was a field service engineer of MRI machines, and left the company in February 2012. During their employment, each of these employees signed an agreement with Phillips-PR containing a confidentiality and non-disclosure clause that prohibited them from using, publishing, or disclosing secret or confidential information "during or after" their employment.[3] Ex. 9 ¶ 1; Ex. 10 ¶ 1; Ex. 11 ¶ 1. Calo testified that Phillips-PR has not authorized Toro, Sumpter, or Bracero to access any of Phillips's proprietary information or tools after leaving Phillips-PR's employment. Nor has Phillips-PR given any such authorization to GIS or any of its employees.

GIS is a Puerto Rico corporation founded by Toro and Sumpter, who were the company's sole stockholders prior to April 2014. *Id.* ¶ A(ii). GIS competes with Phillips-PR, and provides repair and maintenance services to hospitals and healthcare providers. Docket No. 91 ¶ 5. After April 2014, Toro became GIS's sole stockholder. Docket No. 92 ¶ A(iii). General Imaging Services Corporation ("General Imaging") is a Puerto Rico

[3] Calo acknowledged that the agreements signed by Toro, Sumpter, and Bracero did not have a non-compete clause. Ex. 9 ¶ 1; Ex. 10 ¶ 1; Ex. 11 ¶ 1.

corporation founded by Sumpter after he left GIS. *Id.* ¶ A(vii). The inventory of parts for GIS and General Imaging is stored in GIS's warehouse and is "interchangeable" between the two companies. *Id.* ¶¶ A(vi)–(vii). The two companies have also "interchangeably" provided services to the Mennonite General Hospital ("Hospital"), though the obligor on the service agreements with the Hospital has alternated between GIS and General Imaging. *Id.* ¶¶ A(vii)–(xiii).

Servicing of Phillips-Branded MRI Machines

Calo testified that Phillips-PR had a 60-month service agreement with the Hospital that was supposed to run from September 19, 2008 to September 19, 2013. Exs. 8, 15. The Hospital cancelled the service agreement in August 2012, and Calo highlighted that the time period in which the contract was cancelled coincided with the time period when Bracero ended his employment with Phillips-PR. Ex. 16. Before the contract was cancelled, Calo met with the Hospital's administrator, among others, and was told that the Hospital would now go to "GIS Corp. for services."

Orlando Torres-Rodriguez ("Torres") is the director of the radiology department at the Hospital, and is familiar with the persons who provided services to the department's medical equipment. Torres testified that since February 2012, GIS has serviced its Phillips-branded MRI machine and that "GIS Corporate" presently services the machine. Since February 2012, he has seen Sumpter, Toro, and their workers service the Hospital's MRI machine. On cross-examination, Torres was asked whether he had seen Bracero servicing the Hospital's MRI machine. He testified that he did not know a person named Bracero, and that he had not seen this person at the Hospital. He added that he knew *all* of GIS's employees who visited his department and serviced the MRI machine, and that these employees did not include a person named Bracero.

Jose Rivera-Rivera ("Rivera") is the owner of Medical X-Ray ("Medical X-Ray") in Ponce, and is familiar with the persons who service the company's Phillips-branded MRI machine. Since February 2012, GIS has "mostly" serviced Medical X-Ray's MRI machine, though Phillips serviced the machine once or twice. When GIS serviced the machine, Sumpter, Bracero, and Toro were the ones who provided that service. Recently, Alpha Medical has taken over the servicing of the MRI machine. Rivera testified that Bracero works for Alpha Medical and that Bracero has been the "main" servicer of the MRI machine since Medical X-Ray has owned it.

The MRI Machines

Ives Sakuyoshi ("Sakuyoshi"), a magnetic resonance national support specialist for Phillips, is responsible for training and assisting field service engineers in the United States and Canada. These responsibilities include helping a field service engineer during an "escalation," which is a situation where a field service engineer is unable to resolve an issue and seeks additional guidance from the company's national support specialists. According to Sakuyoshi, an MRI machine has three components: (1) the operator's console, where an operator controls the machine by using, among other things, the machine's host computer ("Host Computer"); (2) the admission room, where the machine's magnet is located and the patient is placed; and (3) the technical room, where the machine's equipment is housed. These components were the same for the Phillips-branded MRI machines sold to the Hospital and Medical X-Ray. Ex. 1, §§ 11-3, 11-4; Ex. 2 §§ 11-3, 11-4. Both machines are equipped with Ethernet cards and a remote services network router ("Router"), which permit Phillips to remotely access the MRI machines through an encrypted Internet connection.

Access-Restricted Areas

To service, calibrate, or maintain an MRI machine without using any of Phillips's proprietary information, a customer or non-Phillips representative may use the Basic Level. A Phillips-employed field service engineer has additional tools at his or her disposal to service an MRI machine: embedded on the Host Computer's software is the CSIP Tool, which permits a viewer to access Phillips's proprietary information. The CSIP

Tool, which is not available to the public,[4] has varying tiers of access: Levels 0, 1, 2, and 3. As the level of access increases, the amount of proprietary information available also increases: Level 0 has some restricted information, Level 1 gives "more access," Level 2 is assigned to national specialists and field service engineers, and Level 3 is a "factory level."[5] Phillips assigns an employee a level of access commensurate with his or her training and entitlements; a new field service engineer, for example, may only be granted access up to Level 1. According to Sakuyoshi, Level 2 is "expert" mode and contains the most advanced diagnostic tools that Phillips has spent much effort and resources to develop.

To protect—and restrict access to—the CSIP Tool, Phillips has developed two security solutions: Phillips Medical System Security ("PMSSec"), and Integrated Security Tool ("IST"). One method of accessing the CSIP Tool requires a field service engineer to connect a Smart Card to the Host Computer. A Smart Card is a USB-like device that contains a microchip. The microchip is embedded with a password-protected digital certificate that is issued only with a valid IST account. An IST account, which is issued by Phillips, allows a person to have a username/identification and password (i.e., login credentials).

Another way to access the CSIP Tool is through the MR Response Generator Tool. Under this method, the MRI system sends a challenge to the field service engineer's laptop, the field service engineer types into the MRI system the response to the challenge, and the MRI system then grants access to the CSIP Tool. Access via this method requires

[4] Phillips's General Terms and Conditions of Sale and Software License, which accompany the sale of an MRI machine, provide that the "license does not extend to any maintenance or services software shipped (separately or with the Product) to or located at customer's premises which is intended to assist Phillips' employees or agents in the installation, testing, service, and maintenance of the Product." *See* Ex. 5 at 34 ¶ B.

[5] Sakuyoshi explained that "Level 0" and "Basic Level" are sometimes confused and mistakenly used interchangeably. He clarified the difference: Basic Level provides none of Phillips's proprietary information and is thus referred to as Level -1, while Level 0 provides *some*, though not much, proprietary information.

an IST account, too. None of the tools that are used to access the CSIP Tool are available to the public. But according to Sakuyoshi, it is possible to transfer to others the IST account login credentials, as well as the MR Response Generator Tool, which can be installed on any laptop.

Unauthorized Access to CSIP Tool

On October 20, 2014, Sakuyoshi received a call from a field service engineer in Puerto Rico who was unable to resolve a system problem with Medical X-Ray's MRI machine. After receiving this call, Sakuyoshi asked the local field service engineer to send him the log files for the system. Those files showed some "unusual activities" and indicated that an IST account deactivated in 2012 was being used to access CSIP Levels 0, 1, and 2. Each IST account has a unique identification number that is not reassigned to subsequent employees.

After consulting Phillips's database where all assigned identification numbers are recorded, Sakuyoshi learned that Bracero's deactivated credentials were being used to enter access-restricted areas of the system's software, specifically, CSIP Levels 0, 1, and 2. *See* Ex. 3. The logs for Medical X-Ray's MRI machine indicate that Bracero's login credentials were used numerous times between October 2012 and October 2015 to access CSIP Levels 0, 1, and 2. *See* Ex. 3. Sakuyoshi also learned that the MR Response Generator Tool—as opposed to a Smart Card—had been used to access the CSIP Tool. Phillips began paying attention to the log files of Phillips-branded MRI machines, and discovered that Bracero's deactivated credentials were also being used to access the Hospital's MRI machine. *See* Ex. 4. The log files for the Hospital's MRI machine indicate that Bracero's login credentials were used numerous times between October 2012 and March 2015 to access CSIP Levels 0, 1, and 2. *Id.*

According to Sakuyoshi, these instances of unauthorized access were unprecedented. The only explanations that Phillips has reached—after asking many employees to resolve the issue—is that the MR Response Generator Tool has been "spoofed," or that whoever has obtained access found another way to "circumvent the software protection." The company has not found a solution to the problem because the MR Response Generator Tool is "complex." And while the company has considered removing the MR Response Generator Tool entirely, it is hesitant to do so because the MR Response Generator Tool is used in heavily regulated medical equipment. Sakuyoshi also asserted that the CSIP Tool has been damaged because this application is meant to protect Phillips's intellectual property and the application is not able "do its job" on account of the breaches. He acknowledged, however, that the MRI systems themselves have not been damaged by the breaches into the CSIP Tool.

Phillips hired Enterprise Risk Management ("ERM") to investigate the breaches into the CSIP Tool. ERM conducted a forensic analysis of these breaches, and had been paid $6,000 at the time of the hearing. Michael Burgess ("Burgess") was employed by ERM, prepared a report (which has an addendum), and was qualified to testify as an expert witness as to the matters examined in his report. Exs. 6, 7. Burgess's report explains each of the six columns in the MRI system's log: the first column identifies the user identification number; the second, the date of access; the third, whether the system was accessed locally or remotely; the fourth, the organization that accessed the system; the fifth, the extent of access (i.e., CSIP Levels 0, 1, or 2); and the sixth, any comments that the user entered. Ex. 6 at 3–4.

Burgess confirmed that Bracero's identification number (35914) did not have any authority to access the MRI systems because it had been deactivated as of May 2012, and that someone was using the MR Response Generator Tool with Bracero's identification number to circumvent the CSIP Tool. Ex. 6 at 5; Ex. 2. On cross-examination, Burgess acknowledged that Bracero had returned all the Phillips-issued hardware (i.e., dongles, laptops, and so forth). He explained, however, that the MR Response Generator Tool could run on any laptop.

DISCUSSION

Phillips-PR contends that it is entitled to a preliminary injunction under the CFAA, 18 U.S.C. § 1030(a)(2), as well as under Puerto Rico's Industrial and Trade Secret Protection Act ("Trade Secret Protection Act"), P.R. Laws Ann. tit. 10, § 4136. Docket No. 2. Defendants contend that Phillips-PR is unable to maintain an action under § 1030, but provided no argument whatsoever for denying injunctive relief on the basis of the Trade Secret Protection Act. Docket No. 53.

I. Section 1030(a)(2)

A plaintiff seeking a preliminary injunction must demonstrate "that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Defense Council, Inc.*, 555 U.S. 7, 20 (2008) (Court rejected rule that when "a plaintiff demonstrates a strong likelihood of prevailing on the merits, a preliminary injunction may be entered based only on a 'possibility' of irreparable harm").

A. Likelihood of Success

The "CFAA is primarily a criminal statute," but a private cause of action for damages and injunctive relief is permitted under § 1030(g). *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 n.8 (1st Cir. 2001) (*EF Cultural Travel I*); *see also P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*., 428 F.3d 504, 510 (3d Cir. 2005) ("Employers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system.") (quoting *Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003)).

The statute "lists seven different types of" prohibited conduct that "ranges from trafficking in passwords to knowing and unauthorized access" to protected computers.

P.C. Yonkers, Inc., 428 F.3d at 510. A claim under the CFAA requires "that the defendant violate[] one of the provisions of § 1030(a)(1)-(7), and that the violation involve[] one of the factors listed" in § 1030(c)(4)(A)(i). *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009); *see also* 18 U.S.C. § 1030(g).[6] Thus, to bring a successful action "under 18 U.S.C. § 1030(g) based on a violation of 18 U.S.C. § 1030(a)(2)," Phillips-PR must establish that the defendant: "(1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value." *Brekka*, 581 F.3d at 1132.

1. Protected Computer

The CFAA defines the terms "computer" and "protected computer." 18 U.S.C. §§ 1030(e)(1), (2). *Computer* is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device . . . ." 18 U.S.C. § 1030(e)(1). As courts have noted, the Act's definition of "computer" is "exceedingly broad" and "captures any device that makes use of a[n] electronic data processor, examples of which are legion." *See United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011) (identifying "MP3 players, refrigerators, heating and air-conditioning units," among others, as examples); *see also United States v. Nosal*, — F.3d —, No. 14-10037, 2016 WL 3608752, at *5 n.2 (9th Cir. July 5, 2016) (*Nosal II*) (CFAA applies to "computer networks, databases, and cell phones") (collecting cases); *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005) ("devices with embedded processors and software are [also] covered").

[6] The factors were previously codified at § 1030(a)(5)(B). *Compare Brekka*, 581 F.3d at 1131, *with* 18 U.S.C. § 1030(g), *and Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC,* 774 F.3d 1065, 1072 (6th Cir. 2014).

Moreover, "[i]ndividuals other than the computer's owner" may bring an action under the CFAA because they "may be proximately harmed by unauthorized access, *particularly if they have rights to data stored on [the computer]*." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004) (emphasis added) ("district court erred by reading an ownership or control requirement into the Act," leading it to erroneously dismiss CFAA claim "on the theory that the Act does not apply to unauthorized access of a third party's computer"); *Mitra*, 405 F.3d at 495 ("devices with embedded processors and software are covered" by the CFAA); *Oce N. Am., Inc. v. MCS Servs., Inc.*, 748 F. Supp. 2d 481, 487 (D. Md. 2010) ("Plaintiff correctly cites to *Theofel* . . . for the proposition that it does not need to own the 'protected computer' in order to claim damages for a violation of the CFAA . . . .").

In this case, the evidence adduced at the hearing revealed that a Phillips-branded MRI machine consists of three components: (1) the operator's console, where the machine's Host Computer is located; (2) the admission room, where the machine's magnet is located and the patient is placed; and (3) the technical room, where the machine's equipment is housed. Because the MRI machines are equipped with an actual computer that controls the operation of the machine, these devices are within the ambit of the CFAA. And this is so even though the hardware is owned by the Hospital and Medical X-Ray because "[i]ndividuals other than the computer's owner may be proximately harmed by unauthorized access . . . if they have rights to data stored on [the computer]"—as is the case with Phillips's CSIP Tool, which is embedded on a customer's Host Computer. *See Theofel*, 359 F.3d at 1078. Thus, Philips will likely be able to show that a computer was involved in the alleged CFAA violation.

The Act defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication . . . ." 18 U.S.C. § 1030(e)(2)(B). This broad definition of "protected computer"—a computer affected by or involved in interstate commerce—effectively includes "all computers with Internet access.” *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (*Nosal I*)(en banc); *see also United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015) (same); *United States v. Yucel*, 97 F. Supp. 3d 413, 419 (S.D.N.Y. 2015) (collecting cases) (under the CFAA, “[a]ny computer that is connected to the internet is . . . part of a system that is inexorably intertwined with interstate commerce”) (internal quotations and omitted). And as the Seventh Circuit has explained, “the statute does not ask whether the person who caused the damage acted in interstate commerce; it protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the *computer* is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire.” *Mitra*, 405 F.3d at 496 (emphasis in original).

In this case, Sakuyoshi testified that the MRI machines are equipped with an Ethernet card and a Router that connect the machines to the Internet. This Internet connection permits Phillips to access the MRI machines’ computers from a remote location. Sakuyoshi testified, for example, that in October 2014 he remotely accessed Medical X-Ray’s MRI machine after receiving a call from a field service engineer who was having difficulty resolving an issue with the machine. There was also testimony to the effect that the Hospital’s MRI machine was connected to the Internet until shortly before the preliminary injunction hearing, as that computer’s connection to the Internet had been severed. Thus, Phillips-PR can likely establish that a “protected computer” was involved in the alleged CFAA violation.

2. Intentionally Accessed

The statute requires that the defendant “intentionally” access a computer. 18 U.S.C. § 1030(a)(2)(C). The plain language of § 1030(a)(2)(C), as well as its legislative history, indicates that it does not seek to punish those “who inadvertently stumble into someone else’s computer file or computer data, which [may be] particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer or data file that happens to be accessible from the same terminal." *Valle*, 807 F.3d at 525 (internal quotation marks omitted).

In this case, the logs for the MRI machines reveal that they were *locally*—rather than remotely—accessed multiple times by someone who was using Bracero's login credentials. That it was necessary to circumvent Phillips's security tools in order to access the CSIP Tool indicates that the conduct was intentional and could not have come about inadvertently. And while defendants' counsel homed in on the fact that only Bracero's unique identification number was displayed in the logs, there was some evidence at the hearing from which it can be inferred that Toro and Sumpter likely accessed the CSIP Tool.

As an initial matter, Sakuyoshi and Burgess provided testimony to the effect that the MR Response Generator Tool and Bracero's login credentials could be transferred to other persons. Moreover, Torres—the director of the radiology department at the Hospital—testified that he knew *all* of GIS's employees who serviced the department's MRI machine. He testified that since February 2012, GIS has serviced the Hospital's Phillips-branded MRI machine and that the machine is presently serviced by "GIS Corporate." Since that time period, he has seen Sumpter, Toro, and their workers service the machine. However, Torres's testimony was to the effect that he has not seen a person named Bracero servicing the machine—as he is familiar with *all* the persons who service the machine and a person named Bracero has not been one of them.[7] Because the logs for the Hospital's MRI machine indicate that CSIP Levels 0, 1, and 2 were *locally* accessed multiple times from October 2012 to March 2015, and because Sumpter and Toro (but not Bracero) were seen servicing this particular MRI machine, Phillips-PR will likely be able to show that Toro and Sumpter intentionally accessed the CSIP Tool.

[7] In contrast to Torres's testimony, Rivera testified that he saw Toro, Sumpter, *and* Bracero servicing Medical X-Ray's MRI machine.

Moreover, it is uncontested that GIS, which is spearheaded by Toro, and General Imaging, which is led by Sumpter, have treated their inventory and service contracts interchangeably. In light of this arrangement, both companies have provided service to the Hospital's MRI machine. It is also uncontested that Bracero was working for GIS, either on a contract basis or as an employee, and that his login credentials were used to access the CSIP Tool. Because Phillips will likely be able to show that GIS and General Imaging had *someone* in their employ use Bracero's login credentials to hack into the CSIP Tool for the benefit of these two companies, they are also liable. *See Butera & Andrews v. Int'l Bus. Machines Corp.*, 456 F. Supp. 2d 104, 113 (D.D.C. 2006) (all the cases under the CFAA where vicarious liability was found "involve intentional conduct that was directed or approved by the corporate defendant in order to gain an unfair business advantage at the expense of a competitor.") (collecting cases). And the foregoing is particularly so because Toro and Sumpter were former employees of Phillips-PR who signed the confidentiality and nondisclosure agreement and likely knew the wrongfulness of having GIS and General Imaging use Bracero's deactivated login credentials to access the CSIP Tool.

3. Without Authorization *or* Exceeding Authorized Access

As the Supreme Court recently explained, § 1030 (a)(2)(C) "provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio v. United States*, 136 S. Ct. 709, 713 (2016). The Act does not define "without authorization" or "authorization." *See, e.g.*, *Valle*, 807 F.3d at 523–24. But courts have construed "authorization" to mean "permission or power granted by authority." *Valle*, 807 F.3d at 524 (quoting Random House Unabridged Dictionary 139 (2001)); *see also Nosal II*, 2016 WL 3608752, at *6 ("there has been no division among the circuits on the straightforward 'without authorization' prong of this section"). Unlike the phrase "without authorization," the phrase "exceeds authorized access" is defined by the CFAA. The latter statutory phrase means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

"Over the past fourteen years, six . . . circuits have wrestled with the question" of properly interpreting "without authorization" and "exceeds authorized access," both of which appear more than once in the CFAA, as well as with explaining the relationship between the two statutory phrases. *See Valle*, 807 F.3d at 524. Circuit courts have not agreed as to the circumstances in which a defendant "exceeds authorized access," but the First Circuit has held that an employee "likely" exceeds authorized access if he violates an employer's confidentiality agreement. *See EF Cultural Travel I*, 274 F.3d at 581–84 (former employees who violated confidentiality agreements "likely" exceeded authorized access); *see also Nosal II*, 2016 WL 3608752, at *8 n.11 (collecting cases).

The Second Circuit recently clarified the distinction between the two phrases, explaining that "because 'without authorization' most naturally refers to a scenario where a user lacks permission to access the computer at all, one sensible reading of the statute is that 'exceeds authorized access' is complementary, referring to a scenario where a user has permission to access the computer but proceeds to 'exceed' the parameters of authorized access by entering an area of the computer to which his authorization does not extend." *Valle*, 807 F.3d at 524–525 ("the legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend.").

The Ninth Circuit (en banc) had previously offered a similar explanation: "it is possible to read both prohibitions as applying to hackers: 'Without authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files).” *Nosal I*, 676 F.3d at 858; *see also Valle*, 807 F.3d at 525 (one of the legislative history reports “described one instance of ‘computer crime’ in which an individual ‘stole confidential software by tapping into the computer system of a previous employer from [the] defendant’s remote terminal.’”) (quoting H.R.Rep. No. 98–894, at 3691–92).

Both the “without authorization” and “exceeds authorized access” prongs of § 1030(a)(2) require the court to determine whether the defendant had some sort of authorization. *See* 18 U.S.C. § 1030(a)(2)(c). “Implicit in the definition of authorization is the notion that someone, including an entity, can grant or revoke that permission.” *Nosal II*, 2016 WL 3608752, at *8. The Ninth Circuit has recently explained that proper authorization may sometimes be necessary from distinct persons or entities. *See Facebook, Inc. v. Power Ventures, Inc.,*— F.3d —, No. 13-17102, 2016 WL 3741956, at *7 (9th Cir. July 12, 2016) (defendant “needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers)”). To explain this concept, the Ninth Circuit provided an “analogy from the physical world”:

> Suppose that a person wants to borrow a friend’s jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank's property while armed. In other words, to access the safe deposit box, the person needs permission *both* from his friend (who controls access to the safe) *and* from the bank (which controls access to its premises).

Power Ventures, Inc., 2016 WL 3741956, at *7. And in addition to obtaining authority to access from a *proper* person or entity, the grant of access must also be *validly* granted by that person or entity. *See Theofel*, 359 F.3d at 1078 (rejecting argument that NetGate, a third-party, “authorized” defendants’ access to plaintiffs’ information on NetGate’s server because defendants had gained that consent by engaging in conduct analogous to the common-law tort of trespass).

In this case, defendants have suggested that because Medical X-Ray and the Hospital granted them access to the Host Computer, any hacking into the proprietary CSIP Tool does not violate the CFAA. As an initial matter, it bears repeating that "[i]ndividuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it." *Theofel*, 359 F.3d at 1078. But "*Theofel* is silent with respect to the . . . issue of whether a licensee can consent to give access to the licensed information to another," and at least one court has adopted "the basic premise that a defendant's deceitful conduct can vitiate consent or authorization by a licensee." *ATPAC, Inc. v. Aptitude Sols., Inc.*, No. CIV. 2:10294WBSKJM, 2010 WL 1779901, at *6 (E.D. Cal. Apr. 29, 2010).

Having adopted this position, the *ATPAC* court reasoned that "[t]he door remains open for third-parties to be liable under the CFAA for accessing software programs held on a licensee's computers or servers where the defendant engages in the kind of fraudulent conduct that was present in *State Analysis*." *ATPAC*, 2010 WL 1779901, at *6. In *State Analysis*, the defendant used subterfuge, which consisted of "using user names and passwords that did not belong to it," in order to access the plaintiff's proprietary information. *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009). Likewise, another court has held that the CFAA's "'exceeds authorized access' [language] is broad enough" to encompass situations "where people with some authorized access enter into an area of a computer"—such as "a protected software program not owned, but merely licensed, by the owner of the computer"—in order to "decode" the software and "steal its capacity." *Workgroup Tech. Partners, Inc. v. Anthem, Inc.*, No. 2:15-CV-00002-JAW, 2016 WL 424960, at *24 (D. Me. Feb. 3, 2016).

In this case, the evidence received during the hearing revealed that: (1) the Hospital and Medical X-Ray owned the hardware (i.e., the MRI machines and the Host Computers); (2) the Hospital and Medical X-Ray permitted defendants to use the Host Computers; (3) the Hospital and Medical X-Ray did not know how to access *or* use the

CSIP Tool; (4) the software licensing that accompanied the sale of the MRI machines did not extend to programs like the CSIP Tool; (5) defendants, who were former employees of Phillips-PR, circumvented or spoofed Phillips's security solutions with Bracero's deactivated login credentials in order to access the CSIP Tool; and (6) none of the defendants had any authority whatsoever to access the CSIP Tool during the instances revealed by the MRI machines' logs.

Under these circumstances, Phillips-PR likely cannot establish that defendants accessed a protected computer "without authorization"—because this statutory phrase "most naturally refers to a scenario where a user lacks permission to access the computer *at all*." *Valle*, 807 F.3d at 524 (emphasis added). Sakuyoshi acknowledged during the hearing that non-Phillips representatives or the customer can do *some* of the servicing of the MRI machine so long as they are using the "Basic Level." Because it is uncontested that defendants were authorized by Medical X-Ray and the Hospital to access the Host Computers, and because defendants could have potentially used the "Basic Level" to service the MRI machines, Phillips-PR likely cannot show that the Host Computers were accessed "without authorization." Finding to the contrary, as Phillips-PR has previously urged, would (1) collapse any meaningful distinction between the statutory phrases "without authorization" and "exceeds authorized access," and (2) permit a tech-savvy purchaser of a Phillips-branded MRI machine to be liable under the CFAA for servicing his own MRI machine using the Basic Level.

On the other hand, Phillips-PR *will* likely be able to show that defendants *exceeded* any authorized access they obtained from Medical X-Ray and the Hospital. To explain why this is so, I borrow a modified version of the Ninth Circuit's analogy in *Power Ventures*: while the defendants in this case likely had permission to enter the bank's premises (i.e., the computer), that permission did not allow the defendants to pry open the bank's safe deposit boxes and peruse through or use other people's prized belongings (i.e., Phillips's CSIP Tool). *See Power Ventures, Inc.*, 2016 WL 3741956, at

*7. Put another way, while defendants likely had some authority to access the *computer* (which they obtained from Medical X-Ray and the Hospital), they likely exceeded that authority by hacking into proprietary software—the CSIP Tool (where Phillips maintains proprietary data and files)—without any authorization whatsoever from Phillips. *See Valle*, 807 F.3d at 525; *Power Ventures, Inc.*, 2016 WL 3741956, at *7; *ATPAC*, 2010 WL 1779901, at *6; *Anthem, Inc.*, 2016 WL 424960, at *24.

To be sure, there is some authority that arguably supports defendants' position. *See MCS Services., Inc.*, 748 F. Supp. 2d at 487. In *MCS*, the plaintiff, Océ North America, Inc. ("Océ"), designed, manufactured, sold, and serviced "high volume production printing systems (PPS) for commercial printing functions." *Id.* at 483. Océ employed Brian DeFazio, George Ulmer, and Lionel Verrette as field engineers, in which capacity they serviced the printing systems and accessed the plaintiff's proprietary software. *Id.* To work as field engineers, they signed confidentiality agreements. *Id.* These three employees eventually left Océ to work for its competitor, MCS Services, Inc.—which had a license agreement with Océ that allowed MCS to have "two specifically named engineers to use" software on "two designated laptops to service three designated printers owned by Farmers Insurance in California." *Id.* at 484. Before leaving Océ, defendants allegedly copied Océ's software, which they used while working for MCS. *Id.* Defendants also allegedly circumvented Océ's software to use it while working for MCS. *Id.* Océ filed suit when it discovered that MCS was allegedly servicing printers outside the scope of the license agreement and that MCS was buying printers and modifying their functionality to resell them. *Id.*

Under these circumstances, the *MCS* court dismissed Océ's CFAA claim, holding that "[p]laintiff has not demonstrated that Defendants' access of the laptops or printers was unauthorized, and there is no CFAA violation regardless if Plaintiff permitted them to use its software." *Id.* at 487. The court reasoned that while a plaintiff need not own the computer to assert a CFAA violation, "*Theofel* does not vitiate . . . the need for the access to the computers to be unauthorized by whoever controlled such access." *Id.* And while the plaintiff had alleged "that its software was accessed on laptops and printers," the court further reasoned that there were no allegations in the complaint "that the owners of the laptops and printers, or other person with the requisite authority, denied access such that Defendants' access *was unauthorized or in excess of its authorization.*" *Id.* (emphasis added). And this was particularly so because "most of the laptops and printers alleged to have been accessed belonged to MCS or its employees." *Id.*

The *MCS* court, relying on intra-court authority, has effectively held that the requisite authority is always held by the owner of the computer. *See MCS*, 748 F. Supp. 2d at 487 ("there is no CFAA violation regardless if Plaintiff permitted [defendants] to use its software" in the computers owned by MCS and its employees); *see also Role Models Am., Inc. v. Jones*, 305 F. Supp. 2d 564, 567 (D. Md. 2004) (even if NSU had actively retrieved or "accessed" the information from the principal's computer, rather than passively receiving it from the principal, it was the principal's computer and it was his authorization that was relevant). The *MCS* court's approach is in tension with the approach followed by *ATPAC* and *Anthem*. *See Anthem, Inc.*, 2016 WL 424960, at *24; *ATPAC*, 2010 WL 1779901, at *6.

In determining whether Phillips-PR is likely to succeed on the merits, this court should follow the reasoning of cases like *ATPAC* because they are more in keeping with the intent of the CFAA. As an initial matter, the *MCS* court's approach implicitly ties ownership of the computer to the authority to give access to *both* the computer itself *and* any data or files stored therein—regardless of whether the owner of the computer has any authority to access the data or files. *See MCS*, 748 F. Supp. 2d at 487. This approach strays from the meaning Congress sought to give to the term "authorization." *See Valle*, 807 F.3d at 524–525 ("the legislative history . . . describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend."); *see also Power Ventures, Inc.*, 2016 WL 3741956, at *7 (to act lawfully, defendant "needed authorization *both* from individual Facebook users (who controlled their data and personal pages) *and* from Facebook (which stored this data on its physical servers)") (emphases added).

The *MCS* court's approach also forecloses relief to a plaintiff proximately harmed by a defendant's unauthorized access to a plaintiff's proprietary data or files stored on another's computer when the computer's owner grants the defendant access to the *computer*. *See MCS*, 748 F. Supp. 2d at 487. However, other courts have held that the CFAA does not excuse liability merely because the defendant enlists the help of a third party. *See Power Ventures, Inc.*, 2016 WL 3741956, at *6 ("Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability"); *Theofel*, 359 F.3d at 1073–74 ("A hacker could use someone else's password to break into a mail server [which contains data belonging to the plaintiff] and then claim the [third-party] server 'authorized' his access. Congress surely did not intend to exempt such intrusions—indeed, they seem the paradigm of what it sought to prohibit.").

Moreover, while the contours of the CFAA have developed significantly since *EF Cultural Travel I*, this court is ultimately bound by that case. 274 F.3d at 583–84. In *EF Cultural Travel I*, the First Circuit held that former employees who violated confidentiality agreements "likely" exceeded authorized access "by providing proprietary information and know-how to" the plaintiff's competitor in order to create "the scraper," a tool that mined the plaintiff's website for information. 274 F.3d at 583–84. Based on the evidence adduced at the hearing, Phillips-PR will likely be able to show that Toro and Sumpter—both of whom signed agreements with a confidentiality and nondisclosure clause—breached agreements with Phillips-PR by using confidential information and trade secrets to access the CSIP Tool after ending their employment with Phillips-PR. Thus, the court should find that Phillips-PR will likely be able to show that defendants *exceeded* any authorized access they had.

4. Information & Loss

Section 1030(a)(2) requires that the defendant obtain "information." 18 U.S.C. § 1030(a)(2)(C). Phillips-PR will likely be able to establish that defendants obtained information as a result of their access to the CSIP Tool. Sakuyoshi testified that CSIP Levels 0, 1, and 2 contain proprietary information that is not available to the public. And the logs from the MRI machines reveal that this information was accessed multiple times from the MRI machines. Thus, Phillips-PR will likely be able to establish this element.

Turning to the *loss* element, defendants suggest that the plaintiff must show damage *and* loss to maintain an action under § 1030(a)(2)(C). Docket No. 53 at 18. While § 1030(a)(5)(C) requires that a plaintiff show damage, § 1030(a)(2)(C) does not. *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 439 (2d Cir. 2004). *Loss* "of at least $5,000 in value to one or more persons during any one-year period" is sufficient to maintain an action under § 1030(a)(2)(C). *See EquipmentFacts, LLC*, 774 F.3d at 1072; 18 U.S.C. § 1030(c)(4)(A)(i)(I). The CFAA defines *loss* as "any reasonable cost *to any victim*, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11) (emphasis added).

As one court has noted, "the meaning of 'loss,' both before and after the term was defined by statute, has consistently meant a cost of investigating or remedying damage to a computer, or a cost incurred because the computer's service was interrupted." *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004), *aff'd*, 166 F. App'x 559 (2d Cir. 2006); *see also Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 963–64 (D. Ariz. 2008) (cost that plaintiff incurred in conducting a forensic analysis of the defendant's computer was considered in determining whether the plaintiff had suffered sufficient loss).

EF Cultural Travel I, for example, was decided before the term "loss" was defined by the CFAA, and the First Circuit held that the plaintiff "unquestionably suffered a detriment and a disadvantage by having to expend substantial sums to assess the extent, *if any*, of the physical damage to their website caused by [defendants'] intrusion." 274 F.3d at 585 (emphasis added). In so holding, that court further explained: "That the physical components were not damaged is fortunate, but it does not lessen the loss represented by consultant fees." *Id.*

In this case, Burgess testified that Phillips-PR had paid ERM $6,000 to investigate the breaches into the protected information contained within the CSIP Tool. Sakuyoshi also relayed that he and other employees of Phillips have spent many, many hours attempting to determine how the breaches occurred. This evidence makes it likely that Phillips-PR will be able to establish the *loss* element. *See SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 981 (N.D. Cal. 2008) ("where the offender has actually accessed protected information, discovering who has that information and what information he or she has is essential to remedying the harm" and so such efforts are considered "to be part of the loss for purposes of the CFAA").

Moreover, because the Act protects "any victim," 18 U.S.C. § 1030(e)(11), Phillips's efforts can reasonably be characterized as attempts to determine whether *it* had been a victim of the hacking, particularly because Phillips was connected to the MRI machines via the Internet. *See United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006) ("Although the damage was done to the Aventis computer system, the statute does not restrict consideration of losses to only the person who owns the computer system, and the district court properly instructed the jury to consider losses sustained by IBM in determining whether the statutory minimum was met."); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001) (legislative history makes "clear that Congress intended the term 'loss' to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker"). Thus, the court should find that Phillips-PR will likely be able to establish that it suffered *loss* of at least $5,000 during a one-year period.

B. Remaining Factors

In addition to establishing a likelihood of success on the merits, Phillips-PR must also establish that it is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in its favor, and that an injunction is in the public interest. *Winter*, 555 U.S. at 20. Based on the evidence submitted at the hearing, the court should find that Phillips-PR is able to establish each of the remaining factors.

Phillips-PR is likely to suffer irreparable harm in the absence of the injunction for several reasons. First, Sakuyoshi testified that Phillips has not found a solution to prevent the breaches into the CSIP Tool and may have to consider other options to resolve the problem, such as removing the MR Response Generator Tool. The extent of damages that would result from such an action are likely difficult to quantitate, and irreparable harm may be found in such circumstances. *See, e.g.*, *Register.com*, 356 F.3d at 404. Phillips-PR is also likely to suffer irreparable harm because the breaches into the CSIP Tool allow the defendants to view, and potentially use elsewhere, the intellectual property that Phillips has developed and stored in its CSIP Tool. *See, e.g.*, *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1254 (3d Cir. 1983) ("*jeopardy* to Apple's investment and competitive position caused by Franklin's wholesale copying of many of its key operating programs would satisfy the requirement of irreparable harm needed to support a preliminary injunction") (emphasis added). And to the extent defendants' counsel highlighted that the last instances of access to the CSIP Tool occurred in October 2015 as a way to suggest Phillips-PR will no longer suffer irreparable harm or that the CFAA claim is moot, the argument lacks merit because, as a general matter, "voluntary cessation of a challenged practice" will not moot the litigation. *See City News & Novelty, Inc. v. City of Waukesha*, 531 U.S. 278, 284 (2001).

Under the third factor, the court must balance "the hardship that will befall the nonmovant if the injunction issues . . . with the hardship that will befall the movant if the injunction does not issue." *Mercado-Salinas v. Bart Enterprises Intern., Ltd.*, 671 F.3d 12, 19 (1st Cir. 2011). If the injunction is granted, defendants will be prevented from accessing the CSIP Tool and, therefore, may lose business because their clients depended on them to provide services that require the use of the CSIP Tool. On the other hand, if the injunction is not issued, Phillips-PR will continue to have its proprietary information available for defendants' use. Because Phillips-PR ultimately owns the information stored in the CSIP Tool and defendants do not suggest that they are somehow entitled to access that information, the balance of the equities tips in favor of granting the injunction. And this is particularly so because defendants may continue doing business so long as they do not breach into access-restricted areas of Phillips-branded medical equipment.

The public interest that is referred to under the fourth factor refers to "the public interest in the issuance of *the injunction itself*." *Braintree Labs., Inc. v. Citigroup Global Markets, Inc.*, 622 F.3d 36, 45 n.8 (1st Cir. 2010). This factor tips in Phillips-PR's favor because defendants have accessed Phillips's proprietary information and "Puerto Rico has a strong public interest in preserving the rights of its citizens against the misappropriation and misuse of their property." *Am. Health, Inc. v. Chevere*, No. CIV 12-1678 PG, 2013 WL 5297295, at *7 (D.P.R. Sept. 19, 2013). Indeed, the issuance of the preliminary injunction will serve the public interest by ensuring that proprietary software is not breached in order to provide the defendant with proprietary information that the plaintiff has expended time, money, and resources to develop. Because Phillips-PR has demonstrated that each of the preliminary injunction factors weigh in its favor, the court should grant injunctive relief per § 1030(g) of the CFAA.

II. Trade Secret Protection Act

Phillips-PR also moved for a preliminary injunction under the Trade Secret Protection Act. Puerto Rico's Trade Secret Protection Act provides that "[a]ny natural or juridical person who misappropriates a trade secret shall be held accountable for any damages caused to its owner." P.R. Laws Ann. tit. 10, § 4134. The Trade Secret Protection Act also permits the court to grant injunctive relief: "In all cases in which it is proven that an industrial or trade secret has been misappropriated, the court may issue a preliminary injunction order, *for which the plaintiff shall not be under the obligation to prove irreparable damages*." P.R. Laws Ann. tit. 10, § 4136 (emphasis added). Where a Puerto Rico statute provides for injunctive relief and that relief is "not tied to a showing of irreparable injury or to probability of success in the case on the merits," the court need not make findings as to each of the four factors of the common-law test for affording injunctive relief. *See, e.g.*, *DeMoss v. Kelly Servs.*, Inc., 493 F.2d 1012, 1015 (1st Cir. 1974); *see also Waterproofing Sys., Inc. v. Hydro-Stop, Inc.*, 440 F.3d 24, 33 (1st Cir. 2006).

As an initial matter, defendants provided no argument as to why a preliminary injunction should not be granted under the Trade Secret Protection Act. Even if they had, there was sufficient evidence adduced at the hearing to prove that defendants are misappropriating trade secrets and confidential information. As explained above, there is some evidence that defendants have accessed CSIP Levels 0, 1, and 2 in the MRI machines belonging to the Hospital and Medical X-Ray. Toro and Sumpter each signed an agreement with a confidentiality and nondisclosure provision that prohibited them from using Phillips's confidential information or trade secrets after their employment. The evidence at the hearing was to the effect that Toro and Sumpter have created companies—GIS and General Imaging—that compete against Phillips-PR and use trade secrets developed by Phillips. Thus, Puerto Rico's Trade Secret Protection Act provides an alternative basis for granting injunctive relief to Phillips-PR, and the court should grant that relief.

CONCLUSION

For the foregoing reasons, the court should **GRANT** injunctive relief to Phillips-PR—as is permitted by the CFAA, 18 U.S.C. § 1030(g), and the Puerto Rico Industrial and Trade Secret Protection Act. P.R. Laws Ann. tit. 10, § 4136.

This report and recommendation is filed pursuant to 28 U.S.C. § 636(b)(1)(B) and Rule 72(d) of the Local Rules of this Court. Any objections to the same must be specific and must be filed with the Clerk of Court **within fourteen days** of its receipt. Failure to file timely and specific objections to the report and recommendation is a waiver of the right to appellate review. *See Thomas v. Arn*, 474 U.S. 140, 155 (1985); *Davet v. Maccorone*, 973 F.2d 22, 30–31 (1st Cir. 1992); *Paterson-Leitch Co. v. Mass. Mun. Wholesale Elec. Co.*, 840 F.2d 985 (1st Cir. 1988); *Borden v. Sec'y of Health & Human Servs.*, 836 F.2d 4, 6 (1st Cir. 1987).

IT IS SO RECOMMENDED.

In San Juan, Puerto Rico, this 15th day of August 2016.

S/ Bruce J. McGiverin

BRUCE J. MCGIVERIN
United States Magistrate Judge